EXHIBIT A

Lucent Technologies
Bell Labs Innovations

INTELLECTUAL PROPERTY – LAW

Subject: **Patent Submission**
(IDS) No121218
Secure Wireless Network Communications

date: [redacted]

from: **Donald P. Dinella**
Corporate Counsel
Intellectual Property – Law
MH 3B-523
(908) 582-5082
dinella@lucent.com

S. Branigan:
W.R. Cheswick:

The above-identified patent submission, of which you appear to be an originator, was submitted on [redacted] to consider its patentability.

We at IP-Law are committed to being as responsive as possible regarding each submission. However, the volume of patent submissions into IP-Law continues to increase at a significant rate. Moreover, the actual time required to prepare a patent application based on your submission is affected by a variety of factors. As a result, it may take six months or longer before your application is filed with the U.S. Patent and Trademark Office.

The assigned attorney may be an outside attorney retained by Lucent. Should this be the case, I will be the Lucent managing attorney responsible for the application. As such, I will supervise the preparation of the application as required and will be available for consultation as necessary.

Please notify me of any changes in either the technical or commercial aspects of the disclosure. It is also important that I be informed of any relevant work or products by others, whether or not within Lucent, which may utilize this subject matter. In addition, any disclosure to others outside of Lucent may compromise our ability to obtain patent protection. Therefore, please notify me well in advance of any such disclosure, electronic or otherwise.

The booklet, "A Quick Guide to the Patenting Process At Lucent Technologies" may prove helpful. Therefore, if our records indicate that you have not already recently received this booklet, I am enclosing a copy. If you should desire another copy of the booklet, please contact Margaret Rao, at 908-582-2810 or margaretrao@lucent.com.

If you have any administrative questions, please do not hesitate to contact my secretary, Anna Brazil, at 908 582-6925 or abrazil@lucent.com. For substantive issues regarding the submission, please feel free to contact me directly.

Donald P. Dinella

cc: R. Sethi

5. PRESENT STATE OF THE ART

Briefly describe the closest already-known technology that relates to the invention. This would include, for example, already existing products, methods or compositions which are known to you personally or through descriptions in publications or patents.

Virtual Private Network Technology is a well known technology that relates to the Invention

Dynamic Host Control Protocol is a well known technology that relates to the Invention

Wireless Data Networking is a well known technology that relates to the Invention

However, until now, no one has been able to successfully combine these technologies in such a way as to provide a secure, robust wireless data betworking solution.

6. ADVANCEMENT IN STATE OF THE ART

Briefly describe the unique advancement achieved by the invention. This may be done, for example, by describing a problem with the prior art that is solved or specific objects that are achieved by the invention.

Wireless data networking was previously secured by having all users share a single password or small set of passwords amongst themselves. While this strategy provides for security on initial deployment of a wireless data network, it quickly degrades to an insecure network as users are added or leave the network. Logging in this system is non-existant.

This invention allows for secure wireless data networking by through the SBserver, which will perform security functions on behalf of the end users in a wireless data network. It will handle the user authentication. Successfully authenticated users are granted access to the secure data network via encrypted wireless data networking. This robust system easily adjusts to new user additions and the removal of users without compromising the security of the entire system.

This system also has the ability to provide logging, and provide for network consumption control on a per-user basis.

7. HOW ACHIEVED

Briefly describe the invention and how it achieves the advancement described in paragraph 6.

A tradional wireless data network now is connected to a corporate network through the SBserver, which provides temporary data networking connectivity sufficient for authentication using DHCP. A wireless user MUST establish a VPN connection to the SBserver. The SBserver will perform user authentication, consulting a corporate remote authentication database. Upon a successul authentication, the SBserver, using VPN technology, will distribute a unique session encryption key to the user. Wireless connectivity will be secured using this unique session key.

8. DISCLOSURE OUTSIDE OF LUCENT

Anticipated Publication Date:_____ Publication Name:_____

Submitted to Publication Clearance? ☐ Yes ☐ No

If the invention was or will otherwise be disclosed to any non-Lucent employee, describe to whom (person/company), when, where, why, and whether it was/will be under a non-disclosure agreement.

Information disclosed herein is solely for the purpose of initiating a patentability study and may not correspond to any claim(s) of any patent that ultimately issues as a result of the submission of this form.

9. DISCLOSURE TO ANOTHER LUCENT ATTORNEY

Have any of the submitters discussed this matter with another Lucent Attorney? If yes, please identify Attorney:_ _____

10. SUBMITTER #1: _____
Signature Date

SUBMITTER #2: _____
Signature Date

SUBMITTER #3: _____
Signature Date

Providing secure wireless network communications.

Steven Branigan
sbranigan@research.bell-labs.com

Bill Cheswick
ches@research.bell-labs.com

Abstract

Recently there have been great improvements in wireless data networking components. Obtaining wireless data networking cards capable of access speeds of over 2Mbs makes wireless data networking much more desireable for use.

Currently there is insufficient security in the wireless data networking equipment. Therefore, we propose a wireless data network design that allows for a flexible, secure wireless network to be deployed through the use of the SB-server.

We provide a "real-world" example of how we have deployed a secure wireless network for the UNIX room and green room in Murray Hill.

Introduction

Recently there have been great improvements in wireless data networking components. It is now possible to obtain wireless data networking cards that are capable of transmitting over 2Mbs up to 500 meters [1], with higher speed cards on the horizon. Wireless data networking is very popular because it is relatively easy to deploy and allows computing mobility. After all, it can be significantly less cable to run.

However, we notice that a wireless data network does not increase traditional security versus a wired network. The flexibility that makes a wireless network popular also presents some interesting security challenges. Wireless data networking is not point to point such as with a fixed cable. Instead, the wireless signal is broadcast across a footprint, or across multiple footprints. In fact, it is difficult to see the extent of the coverage of a wireless network footprint, and this leads to potential security issues. The risk that a malicious individual can now eavesdrop the network traffic increases because this attack could be performed over a greater area.

Wireless data networking hardware providers attempt to address the security issues through constructs that will limit access to the wireless data network or provide security via end to end encryption. We reason that these tools are too complex to scale well, and that the wireless data networking components will now be objects of attack themselves.

We solve this problem of secure, robust wireless communication by abandoning the wirelesss security hardware tools. Instead, we use PPTP (a VPN technology) for securing the wirless network traffic from a wireless client to a wireless base station. PPTP provides both encryption to secure the air interface transmissions and authentication so that only authorized people can use the network.

This mechanism will be easy to maintain and won't decay into an insecure network over time. Using PPTP for authentication allows us to tie into an existing authentication database. Thus, there is no additional need for userid maintenance in order to use this system.

Assumption

This wireless data network design is not currently targeted for standalone systems that require wireless access. We believe that standalone systems, such as UNIX servers, are better served by a direct connection to the network. The clients should be personal computers or workstations where a person can supply authentication information.

The SB server

This server bridges the insecure wireless network with the protected network. It enforces a policy that only authenticated, encrypted traffic from the wireless network will be allowed to transit to the protected network through the use of PPTP.

The wireless clients must be able to reach the SB-server without a router. The SB-server supplies and manages temporary client IP address using DHCP. Temporary IP addresses are used for establishing a connection to the server via TCP/IP.

We draw a clear distinction between achieving wireless connectivity and achieving network connectivity. Notice that we do not prevent any one from achieving a wireless connection to the wireless network. We can do this because the wireless network does not have anything of value. We are now in the position where we can publicly provide the connection information needed to connect to the wireless network. We do no rely on hiding connection information for our network security (which was never a good idea).

We use the WavePOINT-II Access Point as the wireless base station. The WavePOINT-II is a bridge device that bridges wireless Ethernet to 10BaseT Ethernet. Though it supports two different air interface technologies, we concentrate on the IEEE/802.11 implementation. The WavePOINT-II also provides support for deploying multiple WavePOINT-II access points in a network, which makes it easy to increase wireless coverage.

The wireless data network hardware support speeds of 2 Mb/s. Wireless data network card drivers exist for various implementations of Windows and Unix-style operating systems.

The SB-server is based upon the Plan9 operating system [2]. In our test implementation (see figure #1), the address assigned to the insecure interface is 192.168.50.1. The SB-server hands out addresses via simple DHCP in the 192.168.50.0/24 range on the insecure interface only. The routing gateway is set to the SB-server itself.

The SB-server also performs the functions of a PPTP VPN server. This server processes PPTP login requests and ensures that the clients are using 128-bit encryption. For the login process, the PPTP server verifies an authentication attempt by consulting the Plan9 authentication database on the secure interface side. After a

successful authentication the SB-server will supply an internally valid IP address for use by the client.
Wireless clients that wish to attach to this network must have:

- A WaveLAN IEEE/802.11 wireless network card and the proper drivers.
- The network name must be set to "1127 network" for the wireless card.
- The wireless card must request a DHCP address.
- The PPTP 128-bit client software installed.

Examples

Design #1 for an internal Intranet setting

This is the design we are using to provide wireless networking to the UNIX room and green room in Murray Hill. We are concerned that the network traffic may leak into other rooms, possibly even other floors. Requiring all users connecting to the wireless network to authenticate, and to encrypt all traffic over the air interface mitigates this threat. The Plan9 authentication database provides us with a centrally administered user authentication database.
A sample implementation is depicted in figure #1

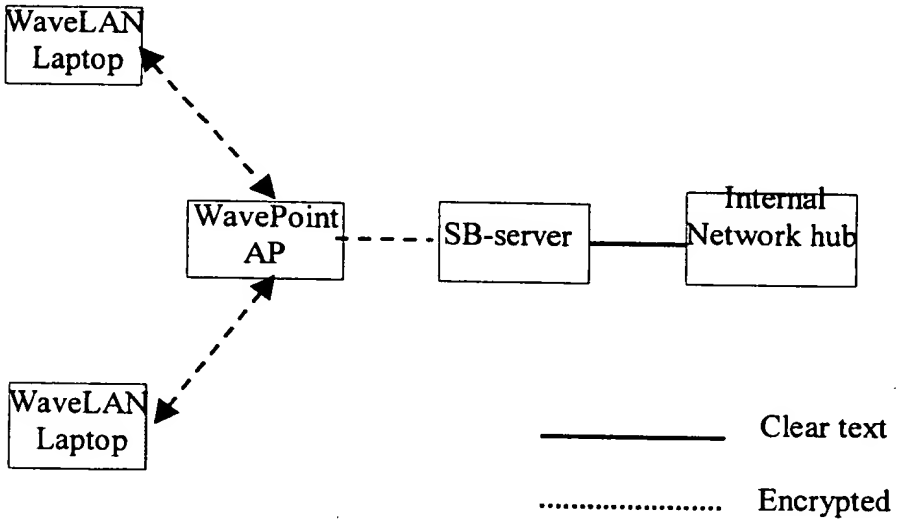

Figure #1

This design can easily handle the addition of other wireless base stations while maintaining the originally engineered security, as in figure #2.

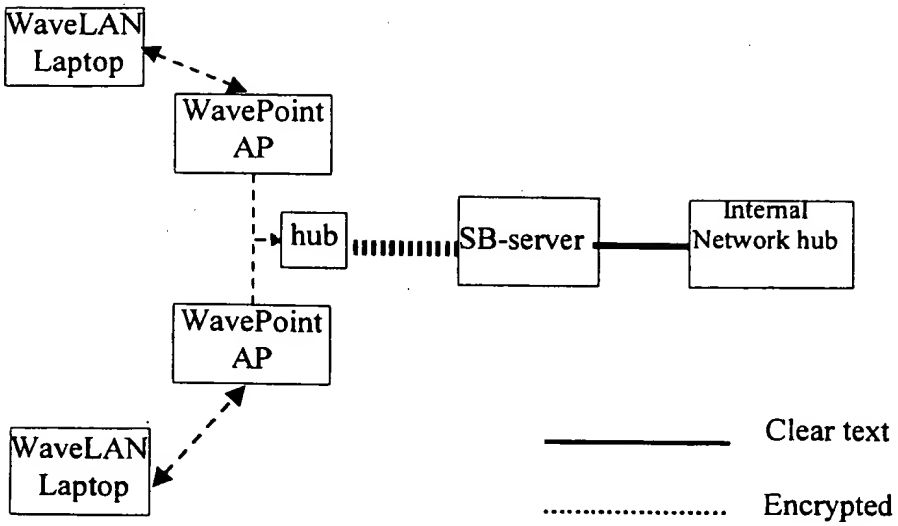

Figure #2

Security analysis

Since the radio footprint is unknown, we must assume that an attacker can eavesdrop, interrupt, hijack, or initiate sessions of their own. Anyone can initiate a session, and we don't care. Though a massive number of connection attempts could swamp our server, this condition would be easily detected, and presumably we could locate the transmitter, which must either be nearby, or extremely powerful.

Although we are relying on Microsoft's authentication protocol, our server forces our clients to use the strong version of the available alternatives [3][see ccs-5, Schneier]. There could be some unknown weakness in the protocol that would allow the attacker to replay a login session. Our server uses a well-tested Plan 9 authentication system for user authentication.

The subsequent communications are protected by Microsoft's implementation of RC-4, with a mandatory 128-bit key. This should be resistant to attack if the protocol is adequate. Microsoft has improved their implementation since [ref Schneier], and the result appears to be more secure [Schneier, personal communication].

Traffic analysis of the clients and encrypted sessions are available to an eavesdropper, since the communications are radiated over a footprint of unknown size. However, since we are using PPTP to encapsulate the traffic, all traffic will have an address tuple of client system and SB-server. Traffic analysis will not yield the addresses of the destination system.

Of course, a client may still be attacked from the network, once connected through the wireless system. These risks are inherent in any network connectivity, and are beyond the scope of this paper.

Logging

Traditional wireless solutions don't use logging, but we require it. Our use of DHCP offers a logical place to record connection attempts, including MAC information. The authentication portion supplies user information.

Conclusions

Implementing security independent of the wireless data network carrier hardware allows us to design and implement secure wireless data networks that are flexible and easy to maintain. We conclude that for large-scale wireless network deployments, the security constructs embedded in most wireless data networking products are difficult to manage and do not scale well. Therefore, we propose that we secure a wireless network with the SB-server, which is built upon currently existing network tools such as DHCP and Virtual Private Network technology. This will create a wireless network that is flexible, easy to manage, and secure.

Our design does introduce another single point of failure (in addition to the network hub), the SB-server. However, the SB-server as a software/hardware component, may have a significantly lower MTBF versus the pure hardware network hub.

Future work

The SB-server provides a way to secure wireless data networking in a corporate setting. Some of the obvious next steps are:

- Using the Lucent VPN Gateway in place of PPTP.
- Address the UNIX/X-windows environment by using SSH in place of PPTP.
- Add the intelligence to the SB-server to prevent the use of temporary addresses that were not assigned by the SB-server. This will limit the amount of interference that a client system can cause with knowledge of the IP address assignment on the insecure side
- Deploy the SB-server at external conferences and trade shows to allow Lucent associates wireless access to the corporate network remotely.

Acknowledgements

I would like to thank Dave Presotto for hearing out the initial design. I would also like to thank Sean Quinlan for his assistance is establishing the proto-type that is currently in use.

S. Branigan **B. Cheswick**

References

[1] http://www.wavelan.com describes the details about the Lucent WaveLan wireless data networking products.

[2] http://plan9.bell-labs.com/plan9/faq.html describes an overview of the Plan9 operating system. It is a good starting point for those who wish to learn more about Plan9.

[3] 5th ACM Conference on Computer and Communications Security (CCS-5), November 2-5, 1998

The Microsoft PPTP 128-bit encryption capable client can be obtained at the following url:
http://www.microsoft.com/downloads/default.asp

SUBMISSION INFORMATION

Attorney: D. P. Dinella

Submission Title: Secure Wirelses Network Communications

Filing Deadline: None

Date Received From Inventor(s): [redacted]

PLEASE SUPPLY WHATEVER INFORMATION IS READILY AT HAND:
(If additional space is needed, please use a second sheet)

INVENTOR: Branigan (Last) Steven (First) (Middle)

SSN (if known):

Organization No.:

BU = Research
Class code II

INVENTOR: Cheswick (Last) William (First) (Middle)

SSN (if known):

Organization No.:

INVENTOR: (Last) (First) (Middle)

SSN (if known):

Organization No.:

INVENTOR: (Last) (First) (Middle)

SSN (if known):

Organization No.:

Please attach all paperwork desired to be bound into folder.

Privileged and Confidential
Attorney-Client Communication

LUCENT TECHNOLOGIES INC.

DISCLOSURE OF INVENTION

THIS DESCRIPTION SHOULD BE SUPPLEMENTED BY ATTACHING COPIES OF RELEVANT DOCUMENTS, SUCH AS TECHNICAL MEMORANDA, PUBLISHED OR TO-BE-PUBLISHED ARTICLES, AND ENGINEERING NOTEBOOK PAGES.
(Also, if for any item there is insufficient space on the form, attach additional pages as necessary.)

DESCRIPTIVE TITLE OF THE INVENTION: Secure Wireless IP Data Networking__

SUBMITTER #1: Steven Branigan — Name (Print)
Bell Labs/Murray Hill, NJ — Company/Location
(908)582-7664/sbranigan@research.bell-labs.com — Phone/E-mail
Eric Grosse — Director's Name

SUBMITTER #2: William Cheswick — Name (Print)
Bell Labs/Murray Hill, NJ — Company/Location
(908)582-7389/ches@research.bell-labs.com — Phone/E-mail
Eric Grosse — Director's Name

SUBMITTER #3: _____ — Name (Print)
_____ — Company/Location
_____ — Phone/E-mail
_____ — Director's Name

2. PRIMARY CONTACT
If more than one Submitter is named above, who will have the primary responsibilities for interfacing with Lucent IP-Law with respect to preparing and prosecuting a patent application for the invention?

Submitter Name: Steven Branigan

3. PRESENT STATE OF THE INVENTION

☐ Manufacture (Product Name _____ Estimated Ship Date _____)

4. GOVERNMENT CONTRACT INVENTION
Was the invention made under a government contract? ☐ Yes ☒ No

Information disclosed herein is solely for the purpose of initiating a patentability study and may not correspond to any claim(s) of any patent that ultimately issues as a result of the submission of this form.

EXHIBIT B

1. A wired network for providing secure, authenticated access to wireless network clients, comprising:

a server connected to a wireless network access point, and having access to the wired network, the server being operative to perform authentication for a wireless client establishing a connection to the server through the wireless network access point, the server performing authentication by examining authentication information transmitted from the client to the server and determining whether or not the authentication information identifies the wireless network client as authorized to gain access to the wired network, the server being operative to establish a connection session upon authentication of a client, the server being also operative to provide the client with a wired network address valid for the connection session upon authentication of the client, the server being further operative to encrypt communications with the wireless network access point, the server being further operative to provide a cryptographic key valid for the connection session to the client upon authentication of the client; and

a user database accessible to the server for use in validating wireless clients.

2. The wired network according to claim 1 and also including a network hub providing connections between the server and additional resources on the wired network.

3. The wired network according to claim 1 and also including a router providing connections between the server and additional resources on the wired network as well as a connection to an additional wired network.

4. The wired network according to claim 2 wherein the server is operative to provide addresses to clients through dynamic host control protocol.

5. The wired network according to claim 4 wherein the server is operative to communicate with a wireless network client using point to point tunneling protocol.

6. The wired network according to claim 5 wherein the server employs 128-bit cryptoprocessing to communicate with the wireless network client.

7. A wireless network for providing secure authenticated communication between clients of the wireless network and a wired network, comprising:

a wireless network access point operative to establish a connection with a server operating as a portal between the wireless network and a wired network, the wireless network access point being operative to conduct communications with the server in order to authenticate wireless network clients as authorized to access the wired network, the wireless network access point being further operative to receive authentication information from one or more wireless network clients and transfer the authentication information to the server in order to allow the server to examine the authentication information for a wireless network client and determine if the information indicates that the wireless network client is authorized to access the wired network, the wireless network access point being further operative to receive a cryptoprocessing key from the server upon authentication of a client and to transfer the key to that client; and

a plurality of wireless network clients operative to establish connections with the wireless network access point, each client being operative to conduct encrypted communications with the server through the access point, to pass authentication information to the network access point in order to indicate to a server communicating with the wireless network and a wired network whether or not the wireless client is authorized to gain access to the wired network, each wireless network client being further operative to receive address information and cryptoprocessing data from the network access point upon authentication by the server in order to allow communication

with the wired network, each client being operative to conduct encrypted transfer of data to and from the wired network through the access point upon receiving the address and cryptoprocessing information.

8. The wireless network of claim 7 wherein the access point communicates with the server using point to point tunneling protocol.

9. The wireless network of claim 8, also including a hub connecting the wireless network access point and a plurality of additional network access points, each additional network access point communicating with a plurality of additional wireless network clients, the wireless network access point and the additional network access points being operative to establish connections with the server through the network hub.

10. A method of secure communication between wireless network clients and a wired network, comprising the steps of:

establishing a connection between a wireless network access point and a security base (SB) server connected to the wired network;

establishing a connection between the SB server and a wireless network client communicating with the SB server through the wireless network access point;

exchanging encryption keys between the SB server and the wireless network client;

transmitting authentication information from the wireless network client to the SB server through the wireless network access point;

performing authentication for the wireless network client by examining the authentication information to determine if the wireless network client is authorized to gain access to the wired network;

if authentication fails, rejecting connection to the wired network; and

if authentication passes, accepting connection to the wired network, providing a temporary wired network address and a unique session encryption key to the wireless network client and providing access to wired network resources in response to requests by the wireless network client.

11. The method of claim 10 wherein the step of rejecting connection to the wired network is accompanied by a step of logging the rejection and wherein the step of accepting the connection is accompanied by a step of logging the acceptance.

12. The method of claim 11 wherein the step of providing a temporary wired network address to the wireless network client includes using dynamic host control protocol to provide the address.

13. The method of claim 12 wherein communication between the wireless network client and the wired network server is performed using point to point tunneling protocol.

14. The method of claim 13 wherein the step of performing authentication for the wireless network client includes transferring authentication information between the wireless network client and the SB server and wherein the authentication information is encrypted using public key cryptography.

15. The method of claim 14 wherein the step of providing a unique session encryption key includes encrypting the unique session encryption key using public key cryptography.

EXHIBIT B

--rw-rw-r-- M 263271 sys ndb 43499 [redacted] local-cs